International Journal of Security and Its Applications
Vol. 10, No. 1 (2016), pp.203-214
http://dx.doi.org/10.14257/ijsia.2016.10.1.19

A Zero-Watermark Scheme for Identification Photos based on QR Code and Visual Cryptography

De Li[1], Zhe Liu[1] and LiHua Cui[2*]

[1]*Department of Computer Science, Yanbian University*
133002, Yanji, China
[2]*College of Economics and Management, Yanbian University*
133002, Yanji, China
**2732677@163.com*
leader1223@ybu.edu.cn, 827901453@qq.com

Abstract

This paper proposes a zero-watermark scheme for identification photos based on QR code and visual cryptography. The method makes no changes to original images while embedding the QR code watermark. In order to ensure the security, we use Arnold transformation to scrambling the watermark. In the scheme, we use discrete wavelet transform and matrix norm computing to generate the invariant feature values against print-scan attacks. Then the VC scheme is applied to generate the secret image from the feature values and the disturbed watermark by using a codebook. In the extraction scheme, we get the secret image which is registered to certification authority and the feature values extracted from the examined image with VC scheme, and then apply inverse Arnold transformation to restore the watermark, finally repair position patterns of the QR code.

The experimental results show that the proposed algorithm is effective and robust against attacks such as JPEG compression, add noise, multiple filters, scale, little angle rotation and crop, especial print-scan attacks.

Keywords: *Zero-watermark, identification photos, Matrix norm, Visual Cryptography, Print-scan, QR code*

1. Introduction

With the rapid development of information technology, the use of high-tech digital equipment for illegal forgery of activities is also rampant. How to protect the copyright of digital works has the important significance and the extensive application value, especially to the certificate security. Most of the current certificate anti-counterfeiting methods are using watermarking technique, having good robustness for print-scan attacks is one of the most important standards. With regard to certificate anti-counterfeiting watermarking technique, researchers keep on focusing on improving the capacity to against print-scan attacks.

C. Y. Lin stands as one of the early researchers in the field, who models the print-scan process by considering the pixel value and geometric distortions separately [1]. K. Solanki proposes a blind decoding method [2]. The selective embedding in low frequencies scheme hides information in the magnitude of selected low-frequency discrete Fourier transform coefficients. The differential quantization index modulation scheme embeds information in the phase spectrum of images by quantizing the difference in phase of adjacent frequency locations. D.Wu presents a robust image hash algorithm, the print-scan resistant method employs Radon transform to its luminance distribution, before the

* Corresponding Author

ISSN: 1738-9976 IJSIA

wavelet extracts the relationship of the different areas from the luminance distribution [3]. T. Y. Ye proposes a watermarking algorithm for print forgery prevention [4]. It conducted DWT on the original image, split its low frequency band into non-overlapping blocks, and conducted singular value decomposition on each block. The zero-watermark sequence was derived from judging the numerical relationship between singular matrix's norm from each block and mean of singular matrix's norm from all blocks. A. Keskinarkaus propose a technique in which a message sequence is mapped to a direction angle of periodic patterns, which are then embedded into an image. Message segments are embedded to permuted triangular areas in the image, where the triangles are the result of tiling the image with a polygon of the watermark is represented in a coordinate system defined with salient feature points and stored as a key [5]. S. Hamid Amiri proposes a blind watermarking method by using 2D-DWT and 1D-DCT. To specify watermarking parameters, they utilize a genetic algorithm to achieve a predefined image quality after watermark insertion. Suitable locations for watermarking are determined by analyzing the effect of a modeling algorithm [6].

We proposed a zero-watermark scheme for identification photos by using QR code and visual cryptography in this paper. Most of the certificates include text information and image information. QR code can encode these information at the same time so it may be used to achieve certificate anti-counterfeiting. The QR code became popular due to its fast readability and greater storage capacity, and it can be used to convey personal identification information. To solve the problem of transparency of the method, we proposed a new zero-watermark method. The wavelet transform and matrix norm computing are combined to generate print-scan invariant values. The visual cryptography and Arnold transformation are also used to achieve the high robustness and security of the watermark.

The rest of the paper is organized as follows: section 2 reviews Arnold transformation, matrix norm and visual cryptography. Section 3 describes the proposed embedding and extracting scheme. Section 4 presents a variety of simulation experimental results, which illustrate the effectiveness of the proposed algorithm. Finally we conclude the paper in Section 5

2. Background

In this section, the concepts of Arnold transformation, Matrix Norm and Visual Cryptography are briefly described.

2.1 Arnold Transformation

The Arnold Cat map [7] is a well-known prototype for chaotic behavior due to hyperbolic structure. The Arnold transformation is based on scrambled digital image into random noise. Suppose that a point (x, y) in a unit square transforms into the other point (x', y'), for a digital image of $N \times N$, the disserted Arnold transformation is defined as:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \left(\mathrm{mod}\, N\right) \tag{1}$$

Where N is the order of the digital image matrix, $x, y \in \{1, 2, \ldots N - 1\}$. Marking digital image in confusion by changing the location of points, considering the iterative transformation can be used in the pixels coordinates, then get the iterative equation:

$$P_{ij}^{n+1} = TP_{ij}^{n} \left(\mathrm{mod}\, N\right) \quad n=0,1,2,3\cdots \tag{2}$$

Where n is the iteration time.

$$P_{ij}^{n} = \left(i, j\right)^{T} \quad i, j \in \left\{0,1,2,\cdots, N-1\right\} \tag{3}$$

Based on Arnold transformation, a digital image is scrambled to be random noise and the iteration time is the key of the encryption.

2.2 Matrix Norm

In mathematics, a matrix norm is a natural extension of the notion of a vector norm to matrices [8]. Let $A^{m \times n}$ denote the matric with *m* rows and *n* columns. The Frobenius norm or the Hilbert-Schmidt norm can be defined as follows:

$$\|A\|_F = \sqrt{\sum_{i=1}^{\min\{m,n\}} \sigma_i^2} = \sqrt{\operatorname{trace}\left(A^* A\right)} = \sqrt{\sum_{i=1}^{m}\sum_{j=1}^{n} \left|a_{ij}\right|^2} \quad (4)$$

Where A^* denotes the conjugate transpose of A, σ_i are the singular values of A. The norm has the useful property of being invariant under rotations.

2.3 QR code

QR code is the trademark for a type of matrix barcode first designed for the automotive industry in Japan [9].QR code can encode in much type of characters such as numeric, alphanumeric character, symbols, binary, and control codes.

QR code is a matrix symbol that contains of an array of nominally square modules arranged in an overall square pattern, see Figure 1, QR code includes unique finder pattern located at three corners of the symbol and intended to assist in locating its position, size and inclination easily. A wide range of size of symbol is provided for together with four levels of error correction.

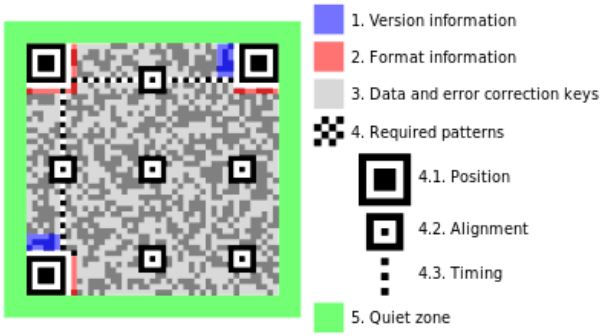


Figure 1. Schematic Diagram of QR Code Structure

2.4 Visual Cryptography

It is a secret sharing scheme that allows a secret to be shared among a set of participants. For this reason, *VC* as a kind of lossless watermarking, which achieves requirements of robustness, imperceptibility, security, blindness, and unambiguity by utilizing the codebook to divide an image into several different sharing images, is widely used in many digital watermarking schemes [10].

Considering the convenience and security of the scheme, in this paper, we adopted a (2, 2) *VC* method. A secret image is just divided into two shares and each secret pixel of an image is replaced by 1×2 pixels. In addition, the secret image can be recovered by stacking the two sharing images. To generate a secret image, the critical step is to make a codebook of *VC* technique. The codebook is shown in Figure 2. Combining the feature image and watermark image, the secret image can be generated by them according to the codebook.

Feature value	mod(*i*+*j*,4)	W(i, j)=1 □ Public	W(i, j)=1 □ Secret	operation	W(i, j)=0 ■ public	W(i, j)=0 ■ Secret	operation
	0						
F(*i*, *j*)=1	1						
□	2						
	3						
	0						
F(*i*,*j*)=0	1						
■	2						
	3						

Figure 2. Codebook used in the Visual Cryptography Scheme

3. Proposed Zero Watermarking Scheme

3.1 Watermark Embedding Process

Figure 3 shows the process of the embedding scheme. The main steps of the embedding procedure are described as follow:

Step1: Watermark image preprocessing

(1) Select the QR Code with 64× 64 pixels as a binary image watermark.
(2) Apply Arnold transformation described in 2.1 with key1 to the watermark.
(3) Step2: Cover image preprocessing
(4) Select an identification (ID) photo with 512 × 512 pixels as the cover gray image.
(5) Decompose the cover image into seven sub-bands by 2-level DWT and extract the sub-band LL of the image.
(6) Divide the image into 4 × 4 blocks, compute the Frobenius norm of each block matrix and the mean value of them, if it's value is bigger than the mean value, we define the value of that block as 1, otherwise, define that block as 0. So the feature image is generated.

Step3: Employ *VC* technique described in 2.3 to generate the secret image from the feature image and the disturbed watermark according to the codebook, and then register the image to certification authority (*CA*).

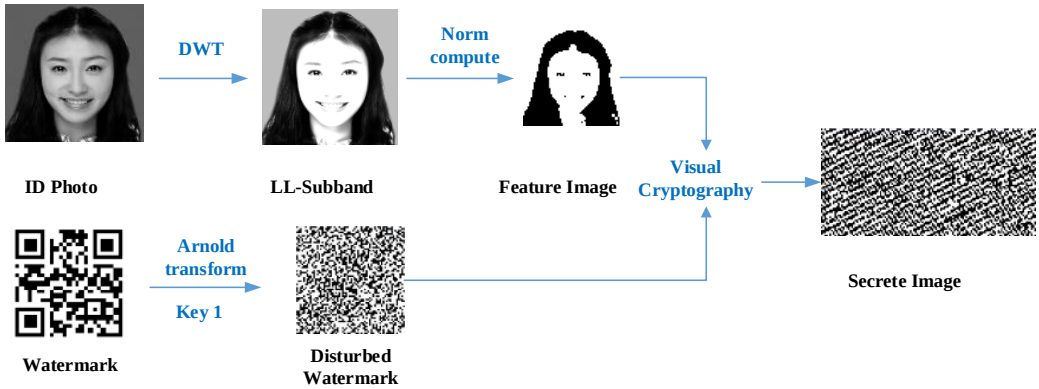


Figure 3. Process of the Embedding Scheme

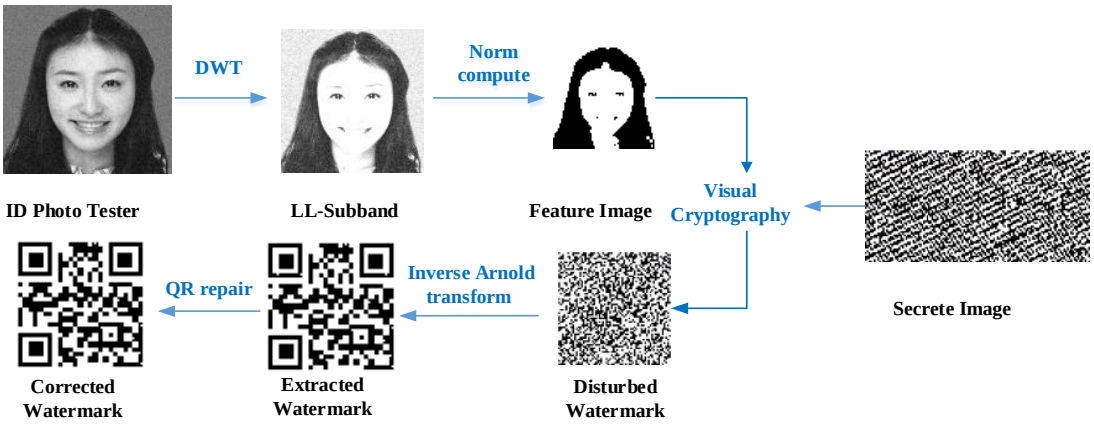


Figure 4. Process of the Extraction Scheme

3.2 Watermark Extraction Process

The extraction process is similarity to the embedding process. Figure 4 shows the process of the extraction scheme. The main steps of the embedding procedure are described as follow:

Step1: Get the secrete image from *CA*.

Step2: Suspected image processing

(1) Decompose the test identification photo into seven sub-bands by 2-level DWT and extract the sub-band LL of the image.

(2) Divide the image into 4 × 4 blocks, compute the Frobenius norm of each block matrix and the mean value of them, if it's value is bigger than the mean value, we define the value of that block as 1, otherwise, define that block as 0. So the feature image of test photo is generated.

(3) Generate a public image by feature image according to the codebook.

Step3: restructure the disturbed image from secret image and public image.

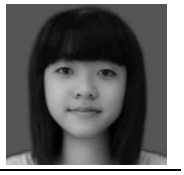
Step4: Do the inverse process of Arnold transformation with *key1* to get the extracted watermark.

Step5: repair the position patterns of the QR code.

4. Experiment Results and Analysis

In this experiment, a size of 64 × 64 binary QR Code image is taken as the owner information. The test cover gray images are all identification photos size of 512 × 512. The PPI (Pixel per inch) of these photos is 300 and the capacity is 257 KB. The cover image and watermark image are shown in Table 1.

Table1. The Cover Image and Watermark Image

					
Watermark	No.1	No.2	No.3	No.4	No.5

4.1 Common attacks

The common attacks are listed in Table 2.

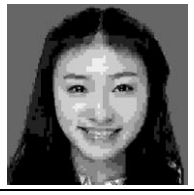
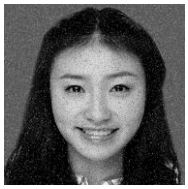
Table 2. A Summary of the Common Attacks

Types	Contents	Types	Contents
JPEG compression	Quality = 0	Scaling	Reduce or enlarge
Salt & pepper noise	Noise density = 0.05	Crop	Crop the image
Gaussian noise	Variance = 0.05	Rotation	Method = 'crop'
Histogram Equalization	Use the histogram to enhance the image	Gaussian low-pass filter	16× 16 Gaussian filtering
Brighten	Add 30 on each pixel value	Darken	deduct 30 on each pixel value

In this paper, bit correction rate (BCR) measures the similarity between an original watermark W and the extracted watermark W′ . High BCR values indicate the algorithm is more robust. The BCR is defined by

$$BCR(W,W') = 1 - \frac{\sum_{k=1}^{m} |W_k - W'_k|}{m} \quad (5)$$

The Figure 5 lists the results under the multiple attacks while using image No.1. The experiment results show that the method is robust to most of common attacks, especially to JPEG compression, filter and add noise attacks. For darken image and brighten image attacks, the brightness of each pixels has changed which makes big pixel distortion of image, even though, the QR code still can be identified. For the geometry distortion attacks such as rotation and crop image which may cause the QR code can't be identified.

Content	Attacked image	Extracted watermark	Content	Attacked image	Extracted watermark
Attack free			Brighten		
JPEG quality 0			Darken		
Salt & pepper noise 0.05			Rotation 5º		
Gaussian noise 0.05			Scaling 0.25		

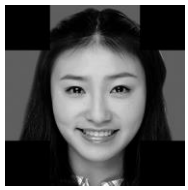
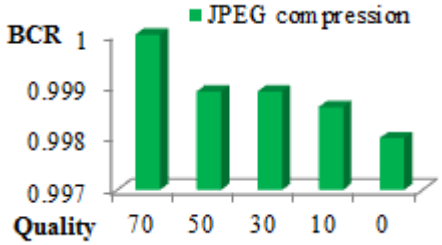
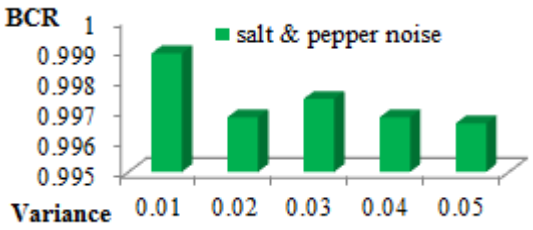
Histogram equalization			Center crop 1/16		
Gaussian low-pass filter			Corner crop 1/4		

Figure 5. The Results under the Multiple Common Attacks while using Image No.1

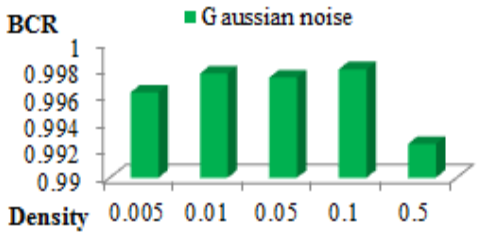
The Figure 6 lists the BCR values response for multiple attacks while using image No.1. In the figure, the green color indicates that the extracted QR code can be identified, and the red color illustrates that the extracted QR code can't be identified. The results show that the method is robust to these attacks by using ID photo image No.1.



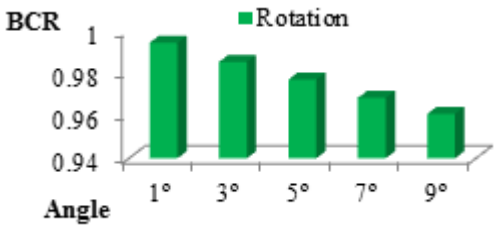
(a) JPEG Compression



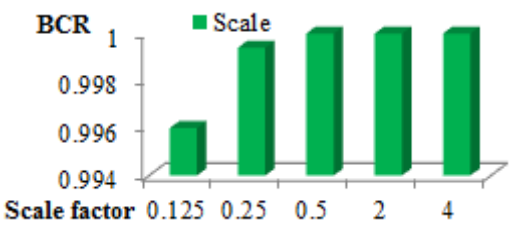
(b) Salt & Pepper Noise



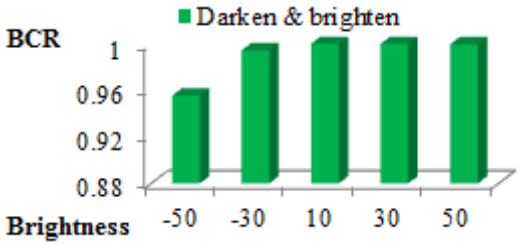
(c) Gaussian Noise



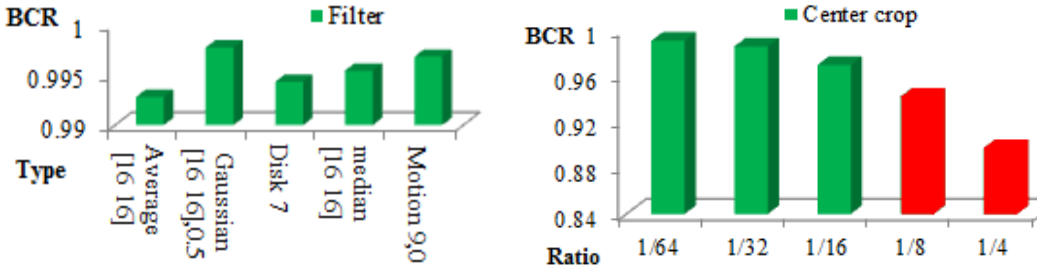
(d) Rotation with Crop



(e) Scale then Restore



(f) Darken or Brighten



(g) Multiple Filter (h) Center Crop

Figure 6. The BCR Values Response for Various Attacks

Figure (a) test the robustness of the method for JPEG compression attack with quality factor 70,50,30,10 and 0. When the factor is 0, the capacity of the compression image is only 3.84 KB. But the BCR value is higher than 0.997.

Figure (b) and figure (c) test the robustness of the method with regard to different kinds of noise, salt & pepper noise with variance range from 0.01 to 0.05 and add Gaussian noise with density from 0.005 to 0.5. The results indicate that the method is robust to add noise attacks.

Figure (d) test the robustness of the method for rotation attack. To make the attacked image the same size as the original image, we crop the rotated image to fit. Considering that the cover images are ID photos which used in the credentials, after print-scan operation, they were rotated by small angle. In the experiment, we set angles range from 1º to 9º. When we rotate the image by 10º, the BCR value is low than 0.95 and the QR Code can't be identified. So the method is robust under small angle rotation attacks.

Figure (e) test the robustness of the method for scaling attack. To make the scaled image the same size as the original image, we rescale the scaled image to fit. In the experiment, we set scale factors range from 0.125 to 4. The factor is smaller, the scaled image is fuzzier. When the factor is 0.125, we reduce the image, make its sizes of one eighth of original sizes at first, and then enlarge the scaled image to its eightfold size. The results show that the method is robust under scaling attacks.

Figure (f) test the robustness of the method for darken image and brighten image attacks. In the experience, the brightness value of each pixel is changed. The results show that darken image has more influence on image than brighten image. When we deduct 50 on each pixel value of the image, the BCR value is higher than 0.96.

Figure (g) test the robustness of the method for multiple filter attacks, including Gaussian low-pass filter of size 16 × 16, the liner motion of a camera by 9 pixels, the average filter of size 16 × 16, the circular averaging filter within the square matrix of size 15, the median filter of size 16 × 16. The BCR values show that the method is robust under filter attacks.

Figure (h) test the robustness of the method for center crop attacks. Since the center of the image conveys mainly feature such as face, eyes, nose and mouth of the ID photos. We crop the center of the image by different percentages. When the crop percentage is higher than 1/8, the ID photo can't be identified, and the extracted QR code is also can't be identified.

4.2. Print-Scan Attacks

We test the robustness of the method for once and twice print-scan attacks. The processes of experiment are as following: 1 print the ID photos on A4 paper by using HP LaserJet 1005 with DPI (dot per inch) 600. 2 scan the printed image by using HP Scanjet 5590 with DPI 300. 3 using Photoshop to do crop correction and rotation correction on

scanned image. 4 use bilinear interpolation to make the size of print-scanned image to 512 × 512. The processes of the twice print-scan attack are the same as the once print-scan attack.

Figure 7 shows the results under the print-scan attacks while using image No.1~No.5. From the figure, one can find that the QR code all can be identified after print-scan attacks. That is to say, the method is robustness for once and twice print-scan attacks.

To test the robustness of the method for different ID photos, we select five images No.1~No.5. Figure 8 shows the BCR values under multiple attacks while using these images. From the figure, we can find that the rotation, crop and print-scan attacks have more influence on images than other attacks. Generally speaking, although the rotation, crop and print-scan attacks can cause little distortion of the images, the proposed method is robust to these attacks in an appropriate range.

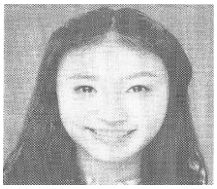
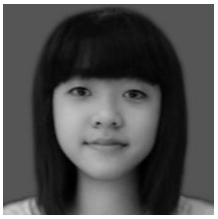
Content	Original image	Print & scan once	Extracted watermark	Print & scan twice	Extracted watermark
No.1					
No.2					
No.3					
No.4					
No.5					

Figure 7. The Results under the Print-Scan Attacks while Using Image No.1~No.5

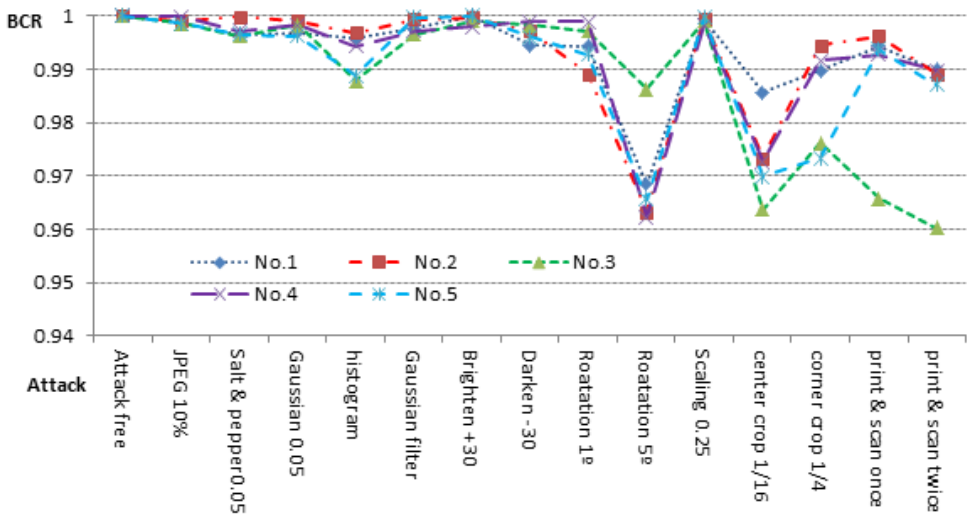


Figure 8. The BCR Values under Multiple Attacks while Using Image No.1~No.5

This paper presented a zero-watermarking scheme. The QR code watermark conveys personal secrete information and it can be easily and quickly identified by evaluator which installed in cellphone. During watermark embedding, it first finds out the print-scan invariant characteristics of ID photos by discrete wavelet transform and matrix norm computing. Secondly the watermark is disturbed by employing Arnold transformation. Finally the visual cryptography is used to generate the secret image for authentication. Although the proposed method still has limitations such as a need for a trusted third party to store the secret images. But it is blind and also has high imperceptibility. Furthermore, it is robust against print-scan attacks.

Acknowledgments

This research project was supported by the National Natural Science Foundation of China (Grant No. 61262090).

Reference

[1] C. Y. Lin and S. F. Chang, "Distortion modeling and invariant extraction for digital image print-and-scan process", presented at the Int. Symp. Multimedia Information Processing, **(1999).**

[2] K. Solanki, "Print and Scan Resilient Data Hiding In Images, in: Proc. of IEEE transactions on information forensics and security", no. 4,**(2006)**, pp. 464-477.

[3] D. Wu, X. B. Zhou, X. M. Niu, "A novel image hash algorithm resistant to print-scan", Signal Processing 89 **(2009**), pp.2415-2424.

[4] T. Y. Ye, "A Watermarking Algorithm for Print Forgery Prevention Based on Comparison between Norm and Mean of Norm", Opto-Electronic Engineering, vol. 38, no. 6, **(2011)**, pp.126-133.

[5] A. Keskinarkaus, A. Pramila, T. Seppänen, "Image watermarking with feature point based on synchronization robust to print-scan attack" J. Vis. Commun. Image R, vol. 23, **(2012)**, pp. 507-515

[6] S. Hamid Amiri, M. Jamzad, Robust watermarking against print and scan attack through efficient modeling algorithm, Signal Processing: Image Communication, vol.29 **(2014)**, pp.1181-1196

[7] V. I. Arnold and A. Avez, Ergodic Problems of classical Mechanics. Benjamin, New York 1968.

[8] http:// en.wikipedia.org/wiki/Matrix_norm

[9] ISO/IEC 18004:2000(E), Information Technology Automatic Identification and Data Capture Techniques Bar Code Symbology QR Code, (**2000**)
[10] D. C. Lou, H. K. Tso and J. L. Liu, A Copyright Protection Scheme for Digital Images Using Visual Cryptography Technique, ScienceDirect, Computer Standards & Interface 29 **(2007)**, pp.125-131

Authors

De Li received the Ph.D. degree from Sangmyung University, major in computer science in 2005. He is currently a professor of Dept. of Computer Science at Yanbian University in China. He is also a Principal Researcher at Copyright Protection Research Institute, Sangmyung University. His research interests are in the areas of copyright protection technology, feature recognition, digital watermarking, and digital forensic marking.

Zhe Liu is a postgraduate, major in Information Security, now studying at Yanbian University in China. Her research interests are in the areas of copyright protection technology, feature recognition, zero watermarking.

LiHua Cui received the Ph.D. degree from KookMin University, major in Financial Management in 2008. She is currently a professor of Dept. of Financial Management at Yanbian University in China. Her research interests are in the areas of Statistical analysis, Information hiding, Pattern recognition, copyright protection technology.